Распространенные способы хищения денег с использованием банковских карт

Способы мошенничества	Чего и зачем добиваются	Способы защиты
Как правило, по телефону от, якобы, сотрудника банка поступает предложение: - обезопасить деньги на счете, переведя их удаленно на защищенный расчетный счет; - реструктуризировать долг по кредиту; - установить программу удаленного доступа (или сторонние предложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки; - зайти в онлайн-кабинет по ссылке на СМС-сообщения или электронного письма, чтобы узнать о проблеме по счету; - включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк.	1.**Напугать** возможностью утраты денег. 2.**Установить доверительный контакт**, что позволит получить: - номер карты; - срок ее действия; - идентификационный код клиента из 3-х цифр, указанных на обороте банковской карты (CVV или CVC-код); - ПИН-код, дающий возможность совершать операции по счету; -код из СМС-сообщения на мобильный номер, к которому привязана банковская карта, что также обеспечит доступ к деньгам на счете. 3. **Похитить деньги**.	1. Не сообщайте звонящему никаких данных. 2.Прервите разговор. 3.Проверьте информацию, связавшись со своим банком по телефону на оборотной стороне карты или на сайте банка. 4.Отслеживайте операции по счету, подключив услугу мобильного банка. 5. При наличии подозрительных операций немедленно звоните в банк. 6.Помните! Банк может инициировать общение с клиентом только для консультации по предложению собственных услуг.